AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

District of the Northern Mariana Islands

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

MARIANAS ENTERPRISES LIMITED ("MEL") office, located on the second floor of the Flame Tree Terrace Office along Isa Drive, Sadog Tasi, Saipan

Case No. MC 17-00014

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See ATTACHMENT A, which is fully incorporated herein.

located in the _____ District of the Northern Mariana Islands , there is now concealed *(identify the person or describe the property to be seized)*:

Evidence of Bringing In and Harboring Certain Aliens, in violation of 8 U.S.C. § 1324(a)(1)(A)(iii), and Unlawful Employment of Aliens, in violation of 8 U.S.C. § 1324a. See ATTACHMENT B, which is fully incorporated herein.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
8 U.S.C. § 1324(a)(1)(A)(iii)	Bringing in and Harboring Certain Aliens
8 U.S.C. § 1324a	Unlawful Employment of Aliens

The application is based on these facts:

See attached Affidavit in Support of an Application for a Search Warrant.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Michael D. Lansangan, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: APRIL 6, 2017

Judge's signature

City and state: Saipan, CNMI

Ramona V. Manglona, Chief Judge
Printed name and title

ESO

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN MARIANA ISLANDS

IN THE MATTER OF THE SEARCH OF MARIANAS ENTERPRISES LIMITED ("MEL") office, located on the second floor of the Flame Tree Terrace Office along Isa Drive, Sadog Tasi, Saipan	CRIMINAL CASE NO. **AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT**

I, Michael D. Lansangan, being first duly sworn, do hereby state as follows:

INTRODUCTION

1. I am a Special Agent (SA) with U.S. Immigration and Customs Enforcement (hereinafter "ICE"), Homeland Security Investigations (hereinafter "HSI"). I have been so employed since December 2010, and have been assigned to the HSI Saipan office in the Commonwealth of the Northern Mariana Islands (hereinafter "CNMI") since July 2011. My training includes completion of the Criminal Investigator Training Program and ICE Special Agent Training Program which I received at the Federal Law Enforcement Training Center in Glynco, Georgia. I have also received extensive classroom and on-the-job training in the areas of general law enforcement, criminal investigative techniques, and criminal law including search and seizure.

2. My duties as an HSI Special Agent include investigating criminal and administrative violations of Federal laws outlined in Titles 8, 18, 19, 21, and 31 of the United States Code (U.S.C.). Investigative techniques that I have relied upon in the course of conducting my investigations include victim, witness, and suspect interviews, review of

documents and records (in paper or digital format) obtained through database checks, subpoena, court order, or consent, and physical and electronic surveillance. I have led or directly participated in over 50 criminal investigations including (but not limited to) investigations related to the unlawful recruitment, enticement, harboring, concealing, and employment of illegal aliens from countries outside the United States, including from the People's Republic of China (hereinafter "PRC"). I have also led or participated in the execution of numerous Federal and State arrest and search warrants. As such, I am familiar with the ways that alien workers may be recruited, brought into the United States and unlawfully employed, and/or concealed or harbored here in the U.S.

3. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing a search of the premises further described in Attachment A and the paragraphs below, and seizure of any evidence found as particularly described in Attachment B and the paragraphs below. The location of the search is the business office of MARIANAS ENTERPRISES LIMITED (hereinafter "MEL"), known to be located on the second floor of the Flame Tree Terrace Office building along Isa Drive, Sadog Tasi village, Saipan, MP, and is described as a white-colored, two-story permanent concrete structure with dark red-colored trim. As further described below, MEL has been linked to BEILIDA OVERSEAS (CNMI) LIMITED (hereafter "BEILIDA"), another company licensed to conduct business in the CNMI. The MEL office is believed to contain several interior work spaces. The public entrance to the MEL office is on the eastern face of the building. A staircase just inside this entrance door leads to the MEL office on the second floor, to the right of the stairs.

4. The facts set forth herein are based on my conversations with, and information received from, law enforcement officers having direct or hearsay knowledge of pertinent facts, my own involvement in this investigation, my review of documents and records generated, maintained, and/or obtained by various local and federal agencies, and information gained through my own training and experience. I have also discussed the facts of this investigation with other law enforcement officials within HSI who have more extensive experience in criminal investigations of unlawful alien harboring and employment than I, and whom shared with me the substance of their experiences in conducting investigations of this nature.

5. Based on my training, experience, and prior discussions with other experienced law enforcement officials within HSI, I am aware that it is generally common practice for businesses to generate and keep records pertaining to clients, vendors, payments, banking and financial transactions, taxes, and employees in their office. These records generally include (but are not limited to) draft and executed contracts, purchase orders, agreements, employee personnel files, invoices, payments made and received, accounts payable and receivable, accounting and payroll ledgers, transaction receipts and duplicates, business checks, and official correspondence to include electronic mail (e-mail). I know that businesses commonly generate or maintain these records in electronic format, using various types of electronic devices including personal desktop computers, laptop computers, personal digital assistants, tablet devices, smartphones, external hard disk drives, memory sticks, and compact discs or DVDs. I am also aware that businesses are able to convert paper records into electronic format through existing software available to the public. Furthermore, these electronic records can be transmitted via the internet using electronic devices such as personal desktop computers, laptop computers, personal

digital assistants, tablet devices, and smartphones, provided the device is connected to the internet.

6. Because this affidavit is being submitted for the limited purpose of securing a warrant to search the described premises, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that evidence of violations of 8 U.S.C. § 1324a and 8 U.S.C. § 1324(a)(1)(A)(iii) are located within the aforementioned premises.

BACKGROUND INFORMATION ON THE CNMI'S PAROLE SYSTEM

7. At all times relevant to the information in this affidavit, and specifically since November 28, 2009, Chinese nationals may be granted permission to enter the CNMI under a parole program. Under the program, Chinese nationals may be paroled only into the CNMI for business or pleasure for a temporary period of time. To be granted parole, an arriving Chinese citizen must a) be a national of the People's Republic of China; b) be solely entering and staying in the CNMI for a period not to exceed forty-five days; c) be in possession of a round-trip ticket that is non-refundable and non-transferable and bears a confirmed departure date not exceeding forty-five days from the date of entry into the CNMI; d) be in possession of a completed and signed Guam-CNMI Visa Waiver Information form (CBP Form I-736); e) be in possession of a completed I-94, Arrival-Departure Record (CBP Form I-94); and f) be in possession of a valid unexpired International Civil Aviation Organization (ICAO)-compliant, machine readable passport. Chinese visitors who are paroled under the program may not engage in local employment or labor for hire, and may not overstay the length of their parole. Any visitor that informs immigration officers at the time of their entry that they plan to work in the CNMI or stay longer than forty-five days will not be paroled into the CNMI.

APPLICABLE LAW

8. Under Title 8 U.S.C. § 1324(a)(1)(A)(iii), a defendant commits the crime of bringing in and harboring certain aliens if there is evidence that proves: First, that there is a person who is an alien; second, that person was not lawfully in the U.S.; third, the defendant knew or acted in reckless disregard of the fact that the alien was not lawfully in the U.S.; and fourth, the defendant harbored, concealed, or shielded from detection the alien for the purpose of avoiding detection by immigration authorities.

9. Under Title 8 U.S.C. § 1324a, a defendant commits the crime of unlawful employment of aliens if there is evidence that proves: First, that the defendant hired, recruited or referred for a fee an alien; second, for employment in the U.S.; and third, while knowing the alien is an unauthorized alien with respect to such employment, or if a defendant: First, hires an alien; second, for employment in the U.S.; third, without verifying that the alien is authorized to work in the U.S.

SUMMARY OF INVESTIGATION

10. The Federal Bureau of Investigation (hereinafter "FBI") initiated an investigation into the death of a PRC national construction worker named Yuanyou HU (hereinafter "HU") in the CNMI. Records revealed that HU entered the CNMI as a tourist under the CNMI-only conditional parole program, and was not authorized to work in the U.S. or the CNMI based on this status. During the investigation, FBI identified BEILIDA OVERSEAS (CNMI) LIMITED (hereinafter "BEILIDA") as the company that hired HU. The investigation further revealed that MARIANAS ENTERPRISES LIMITED (hereinafter "MEL") had oversight of BEILIDA.

PROBABLE CAUSE

11. On March 24, 2017, FBI SA Scott Berkland requested that I conduct a search of HU's immigration status and HU's last entry into the United States. The search of Department

of Homeland Security's (hereinafter "DHS") databases revealed that HU was a citizen of the PRC, and was granted conditional parole entry (e.g., as a tourist) into the CNMI on or about March 7, 2017. Additionally, HU's conditional parole status had expired on March 17, 2017. Based on HU's status as a conditional parolee, HU was not authorized to work in the U.S. or in the CNMI.

12. During the course of their investigation, FBI SA Joe McDoulett informed me of the following facts:

a. On March 22, 2017, the CNMI Department of Public Safety (DPS) received a report from the Commonwealth Health Care Corporation (CHCC) regarding HU's death.

b. On March 27, 2017, Hui LU, a citizen of the PRC, met with CNMI DPS regarding the incident of HU and requested a copy of HU's death certificate in order to send the death certificate to HU's spouse. LU later reported to CNMI DPS that HU had entered the CNMI as a glass contractor for a period of two weeks.

c. On March 28, 2017, LU again met with CNMI DPS and claimed that HU was employed by NANJING BEILIDA NEW MATERIALS SYSTEM ENGINEERING CO. LTD (hereinafter "NANJING BEILIDA"). LU claimed that he (LU) was an employee of NANJING BEILIDA, and the sole owner of BEILIDA. LU stated that BEILIDA was incorporated for the sole purpose of allowing NANJING BEILIDA to operate and conduct business in the CNMI.

d. Also on March 28, 2017, the FBI interviewed Pamela Halstead, Director of Business Licensing at the CNMI Department of Finance, and confirmed that LU

(of No. 1 Shuanglong St., Quinhuai District, Nanjing City, Jiangsu Province, China), is the president and director of BEILIDA. BEILIDA's CNMI business license lists its physical address as Suite 200, Flame Tree Office Terrace, As Mahetog, and its date of incorporation in the CNMI as April 16, 2016.

e. On March 30, 2017, during a Court-authorized search warrant executed by the FBI at the BEILIDA office, the FBI contacted LU by phone to request that he unlock the door to the BEILIDA office. LU complied with the request and shortly thereafter arrived at the office to unlock the door. After unlocking the door and allowing agents to enter and search the office, LU unsuccessfully attempted to open a locked safe located under a desk. LU then called a woman named Hongwei MA (hereinafter "MA") to instruct him how to open the safe over the phone, which failed. LU then requested that MA come to the BEILIDA office in person to unlock the safe, which she did.

f. Upon MA's arrival, FBI agents identified her as a PRC national. MA told the FBI agents that she was an employee of MEL but worked in the BEILIDA office. MA stated that she was responsible for approving all of LU's purchases for BEILIDA. MA opened the locked safe, which FBI agents saw contained several thousand dollars in U.S. currency, several hundred Chinese yuan, as well as employee pay stubs. MA stated that BEILIDA paid all of its expenses in cash, and that the company did not have a local bank account. MA also pointed out her desk and computer, an IBM ThinkPad. On a chair behind MA's desk, SA McDoulett discovered several spreadsheets in Chinese titled "Beilida Complete Personnel Accommodation Statistics Chart." The spreadsheet was accurate to February 7,

2017, and featured a column called "Visa Type," which listed over 150 workers as "hei gong," e.g., the Chinese word for "black worker" or undocumented/illegal worker.

g. FBI agents later received records from U.S. Customs and Border Protection (hereinafter "CBP"), and compared these records with a random sample of names from the BEILIDA list designated "hei gong". Upon comparison, FBI agents confirmed that the individuals whose names were randomly checked against CBP records were in fact conditional parolees, and therefore were not authorized to work legally in the U.S. or the CNMI. FBI agents also confirmed that the entry dates for the individuals on BEILIDA's records matched the entry dates provided in the records from CBP.

13. On April 5, 2017, I conducted a database query on MA and confirmed that she was petitioned by MEL for a CW-1 nonimmigrant transitional worker visa, which was approved by U.S. Citizenship and Immigration Services (hereinafter "USCIS") on December 2, 2016 and is valid until October 23, 2017. In the petition, MEL's mailing address was listed as "PMB 710 Box 10000 Saipan, MP 96950" and the Tax ID number was listed as XXXXX2383. The petition also identified an individual named J[redacted] F[redacted] (hereinafter "F[redacted]") as the point of contact on the petition. While F[redacted]'s job title or position was not identified in the records, I know from prior experience in reviewing similar records that individuals identified as the point of contact for a petition submitted to USCIS are generally owners, management officials, or other specifically authorized individuals representing the petitioning company. I also know from experience that these individuals are oftentimes the same individual actually signing the petition application forms that are submitted to USCIS.

14. On April 5, 2017, SA McDoulett informed me that Qiufang QI (hereinafter "QI", born March 28, 19XX, PRC passport #E10295XXX) and Wencai GUO (hereinafter "GUO", born March 25, 19XX, PRC passport #E68087XXX) were listed as CW-1 visa workers on the "Beilida Complete Personnel Accommodation Statistics Chart" spreadsheets found by FBI agents on March 30, 2017 during execution of the search warrant at BEILIDA. I further learned that QI and GUO were detained at the Saipan International Airport on April 5, 2017 while attempting to depart the CNMI, and were later criminally arrested by FBI agents on probable cause of violating 8 U.S.C. § 1324a and 8 U.S.C. § 1324(a)(1)(A)(iii) relating to this investigation.

15. I conducted a database search on QI and learned that she was petitioned for a CW-1 visa by "MARIANAS ENTERPRISES LTD" which was approved by USCIS on March 28, 2016 and was valid until March 14, 2017. This petitioner's mailing address and Tax ID number were the same as I had previously discovered for MEL while querying MA. I did not find any other records alluding to employment or petition of QI by any other company in the U.S. or the CNMI, including BEILIDA.

16. I also conducted a database query on GUO and discovered that he was also petitioned for a CW-1 visa by "MARIANAS ENTERPRISES LTD" (also with the same address and Tax ID as previously discovered for MEL). GUO's CW-1 visa was approved by USCIS on May 2, 2016 and was valid until April 30, 2017. I did not find any other records alluding to employment or petition of GUO by any other company or entity in the U.S. or the CNMI, including BEILIDA.

17. I also learned from SA McDoulett that on or about March 27, 2017, he and other FBI agents went to the MEL office on the second floor of the Flame Tree Terrace Office

building to identify the BEILIDA office as indicated in CNMI Business License records. SA McDoulett met and interviewed F[redacted] on this date, who informed FBI agents that MEL has been at that location since June 2015. F[redacted] told FBI agents that MEL assists other corporations, including construction contractors, in establishing a footprint in the CNMI to allow those companies to do business here.

18. After speaking with SA McDoulett, I conducted an open-source internet search for J[redacted] F[redacted] and MARIANAS ENTERPRISES LIMITED, and found a result under URL: www.[redacted] which listed J[redacted] F[redacted] as the Administration Officer for MARIANAS ENTERPRISES LIMITED, mailing address: [redacted] Saipan, MP 96950.

19. SA McDoulett also provided me with a photocopy of a document that was discovered and seized from the BEILIDA office area during execution of the search warrant on March 30, 2017. This document was dated January 24, 2017, listed MEL as a "Saipan project construction and hospitality services provider." Another attachment was a flowchart indicating MEL's connection to other companies operating in the CNMI. The flowchart indicated that MEL is to provide construction services to IMPERIAL PACIFIC INTERNATIONAL HOLDINGS LIMITED (hereinafter "IPI"), and that a pending agreement between MEL and IPI would result in MEL paying for construction costs on behalf of IPI and its construction contractors and suppliers, with monthly invoices to be submitted by MEL to IPI for reimbursement.

20. Based on MA's employment with MEL and the scope of her work at BEILIDA, I believe that MEL has an integral business relationship with BEILIDA. Furthermore, I believe that MEL has the ability to exert some measure of control or direction over BEILIDA's

operations and finances. As such, I believe that documents and other evidentiary records relating to BEILIDA's activities and other controlled companies can be found at MEL, to include employees' payroll records, labor invoices, agreements and correspondence.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

22. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

23. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

24. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence

can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

25. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

26. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crime described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on any such devices found because:

27. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

28. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

29. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

30. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

31. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

32. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete

electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

33. *The time required for an examination.* As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

34. *Technical requirements.* Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

35. *Variety of forms of electronic media.* Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

36. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

37. MEL is a functioning company that may conduct legitimate business beyond the scope of that requested in the search warrant. The seizure of MEL's computers may limit its ability to conduct its legitimate business. As with any search warrant, I expect that this search warrant will be executed reasonably, and will likely involve conducting an investigation on the scene of what computers, or storage media, must be seized or copied, and what computers or storage media need not be seized or copied. Where appropriate, law enforcement officers will copy data, rather than physically seize computers, to reduce the extent of disruption. If so requested by employees of MEL, law enforcement officers will, to the extent practicable, attempt to provide the employees with copies of data that may be necessary or important to the continuing function of MEL's legitimate business. If, after inspecting the computers, it is determined that some or all of this equipment is no longer necessary to retrieve and preserve the evidence, the government will return it.

38. Computers or other devices that are seized may be retained by the government for not longer than 60 days, unless that time period is extended by the court for good cause shown. Drives or devices that are imaged by the government will be destroyed or returned to the owner within 120 days of the execution of the warrant, or until the case and any appeal is final,

whichever is longer. The 120-day period may be extended by the court for good cause shown. The government is not required to return any device, information, data or property that is forfeitable as contraband, fruits or instrumentalities of the crime for which conviction is had, or which the government is otherwise permitted by law to retain.

CONCLUSION

39. Based on the facts as set forth in this affidavit, I believe there is probable cause for a search warrant authorizing the search of the premises of MEL, as described in Attachment A, to seek the documents and other items described in Attachment B, under violations of 8 U.S.C. § 1324a and 8 U.S.C. § 1324(a)(1)(A)(iii). I have shown this affidavit and the accompanying search warrant application to Assistant United States Attorney Eric O'Malley, and he informs me that they are in proper form.

Respectfully submitted,

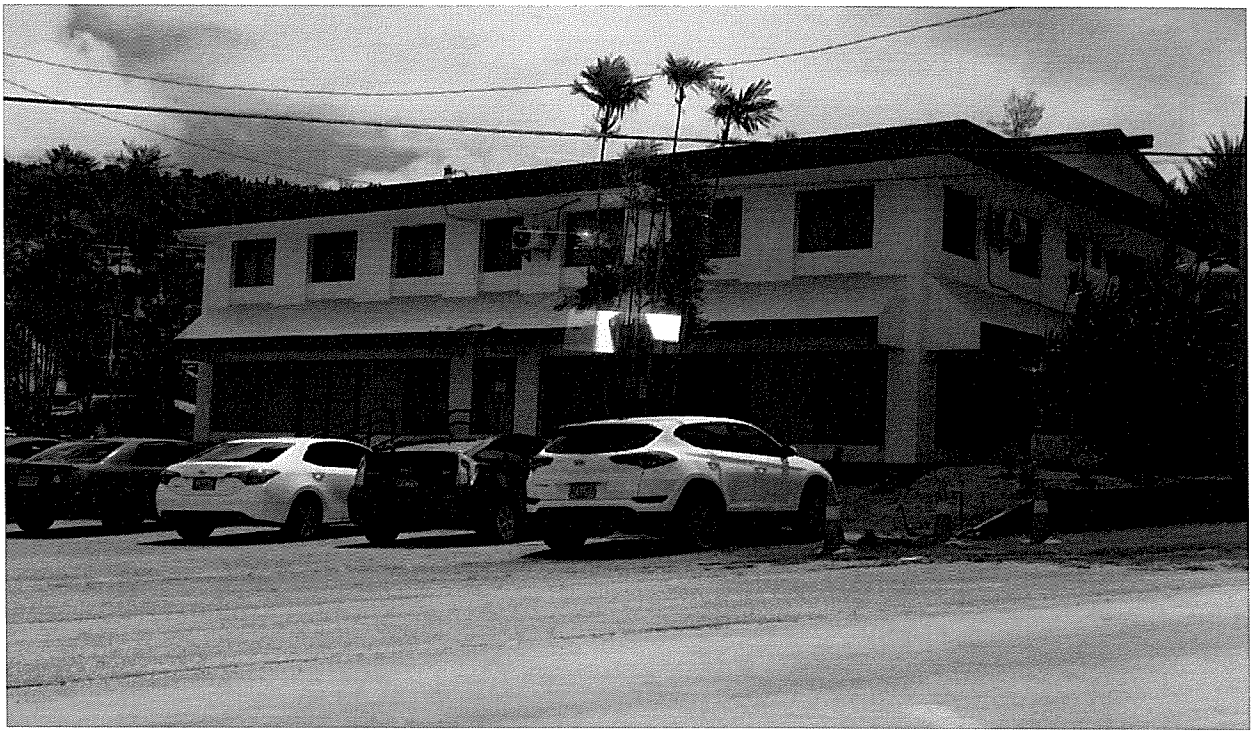
Michael D. Lansangan, Special Agent
Homeland Security Investigations

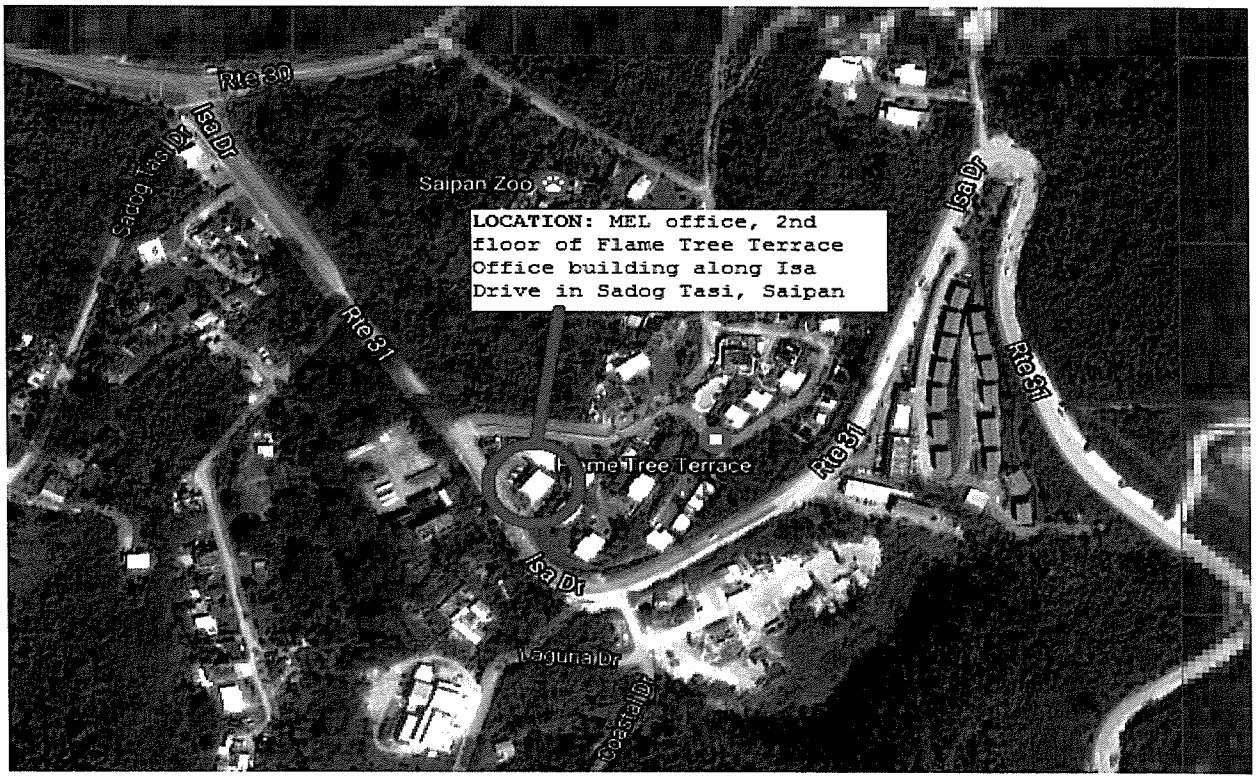
Subscribed and sworn to before me on April 6th, 2017.

U.S. DISTRICT COURT JUDGE

ATTACHMENT A - PROPERTY TO BE SEARCHED

The property to be searched is specifically identified as the MARIANAS ENTERPRISES LIMITED (MEL) office known to be located on the 2nd floor of the Flame Tree Terrace Office building along Isa Drive, Sadog Tasi, Saipan. The building is a two-story, white-colored concrete structure with dark red trim. The entrance door is to the rear (eastern) side of the building, and leads to a staircase up to the MEL office.





ATTACHMENT B - ITEMS TO BE SEIZED

All records relating to violations of 8 U.S.C. § 1324a, Unlawful Employment of Aliens, and 8 U.S.C. § 1324(a)(1)(A)(iii), Bringing In and Harboring Certain Aliens, specifically those violations involving Yuanyou HU, Xiufang QI, Wencai GUO, any other past or present employees of MEL, or any other business operating under MEL, including, but not limited to:

1. Books, records, receipts, ledgers, invoices, contracts, bank statements, money drafts, letters of credit, money orders, cashier checks, bank checks, bank receipts, diaries, notes, correspondence, cash receipts, disbursement journals and spreadsheets, and other documentary records evidencing the harboring, concealment, or employment of illegal aliens;

2. Papers, tickets, notes, receipts, itineraries, passports, identification cards, and copies of aforementioned documents relating to interstate or foreign travel of Yuanyou HU, Xiufang QI, Wencai GUO, or any other foreign national from the PRC relating to the harboring, concealment, or employment of illegal aliens;

3. Address, telephone, or contact information books, and any documents reflecting names, addresses, and/or telephone numbers of past or present employees, business associates, and/or clients;

4. Papers, documents, or other records indicating MEL's business relationship or association to any other businesses or corporations in the CNMI or elsewhere, as they relate to the possible harboring, concealment, or employment of illegal aliens;

5. Employee listings, charts, spreadsheets, ledgers, books, payroll records, payment ledgers, or other records identifying any employee of MEL as relates to the harboring, concealment, or employment of illegal aliens;

6. Records and information relating to immigration documents, specifically any I-129CW petition packets and all supporting documents or information submitted by MEL on behalf of any CW-1 beneficiaries;

7. Indicia of occupancy, residence, and/or ownership of the premises described in Attachment A, including but not limited to utility and telephone bills, canceled envelopes, lease agreements, mortgage records, deeds and titles, registrations, and loan records;

8. Documents, notes, correspondence, communications, and any other papers associated with the ownership, transfer, sale, disposal, or concealment of any asset that relates to a scheme to harbor, conceal, or employ illegal aliens, including but not limited to those in the name of, associated with, of interest to, or under the apparent control of MEL and its officers or employees;

9. United States currency, securities, precious metals, jewelry, automobile titles, financial instruments including stocks and bonds in amounts indicative of the proceeds of harboring, concealing, or employing illegal aliens, and other items of value and/or proceeds of such related activities, as well as access to any locked safes or locked storage containers on the premises and curtilage;

10. Correspondence and relationship records including (but not limited to) letters, faxes, emails, mail, memorandums, invoices, contracts, local and long distance phone records, address books, business cards, and photographs;

11. Fax, typewriter ribbons, correction tapes, printer and copier toner cartridges, and hard drives of copy machines;

12. Any illegal aliens encountered at the location during execution of the search warrant; and

13. Passports, travel documents, or identification of any foreign nationals found during the search which indicate the bearer to be unlawfully present in the U.S. by that date, or which does not bear any indicia of current or valid U.S. immigration status.

For any computer, electronic computing device, or storage medium whose seizure is otherwise authorized by this warrant, and any computer, electronic computing device, or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter "COMPUTER" and "DEVICE"):

1. Evidence of who used, owned, or controlled the COMPUTER or DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat" or other instant messaging logs, photographs, and correspondence;

2. Evidence of software that would allow others to control the COMPUTER or DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

3. Evidence of the lack of such malicious software;

4. Evidence of the attachment to the COMPUTER or DEVICE of other storage devices or similar containers for electronic evidence;

5. Evidence of counter-forensic programs, and associated data, that are designed to eliminate data from the COMPUTER or DEVICE;

6. Evidence of the dates, times, and duration the COMPUTER or DEVICE was used;

7. Passwords, encryption codes or keys, and other access devices that may be necessary to access the COMPUTER or DEVICE;

8. Documentation and manuals that may be necessary to access the COMPUTER or DEVICE, or to conduct a forensic examination of the COMPUTER or DEVICE;

9. Records of or information about Internet Protocol addresses used or accessed by the COMPUTER or DEVICE;

10. Records of or information about the COMPUTER or DEVICE's Internet access and activity, including firewall logs, caches, browser history and cookies; "bookmarked" or saved web pages, search terms that a user entered into any Internet search engine, and records of any user-inputted web addresses; and

11. Contextual information necessary to understand the evidence described in this attachment.

As used above:

1. The terms "records" and "information" includes all forms of creation or storage, including any form of computer, electronic computing device, or electronic storage (such as hard disk drives or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies);

2. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptop computers, tablets, mobile phones, server computers, and network hardware; and

3. The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.